About me

• David Wind (dwind@it-sec.de)
  • Security Consultant at it.sec GmbH & Co. KG
    • Web Application Security
    • Windows Security
    • Social Engineering
  • Privacy enthusiast and bug bounty hunter
    • Acknowledgments: Microsoft, Google, Netflix, …
• Twitter: @slashcrypto
• www.slashcrypto.org

16.11.2018
We are hiring!

• Founded 1996
• Working in more than 30 counties
• New office in Vienna since this year
• Security is our passion – come and join us!
Why ?!
Alexa top 1 million websites

1. google.com
2. youtube.com
3. facebook.com
4. baidu.com
5. wikipedia.org
6. qq.com
7. taobao.com
8. yahoo.com
9. tmall.com
10. amazon.com

Source: https://www.alexa.com/topsites
What we were looking for

• Configuration issues in popular sites with a high security impact
• No fancy stuff
• Easy to find and to exploit
What we found

I'VE SEEN THINGS

TERrible THINGS
What we found

- Subdomain takeover vulnerabilities
- Exposed credentials
- Exposed source code
- CORS misconfiguration
- Exposed AWS S3 buckets
- ....
Where to start?

• We used Alexa top 1 million as input
• Subdomain enumeration using certificate transparency logs
  • crt.sh – they offer Postgres database
    • https://raw.githubusercontent.com/hannob/tlshelpers/master/getsubdomain
  • We discovered around 19 million subdomains
Overview

• Subdomain takeover vulnerabilities
• Exposed credentials
• Exposed source code
• Other interesting things
Overview

• Subdomain takeover vulnerabilities
• Exposed credentials
• Exposed source code
• Other Interesting Things
Subdomain takeover vulnerabilities

- A company points a subdomain to some other domain (e.g. some external Support Ticketing Service) using a CNAME record
- The company stops using the service and forgets to remove the CNAME record
- An attacker claims the domain and gains full control over the vulnerable subdomain
Subdomain takeover vulnerabilities

;; ANSWER SECTION:
subdomain.example.com. 3505 IN CNAME something.trafficmanager.net.
Subdomain takeover vulnerabilities

subjack

Subjack is a Subdomain Takeover tool written in Go designed to scan a list of subdomains concurrently and identify ones that are able to be hijacked. With Go's speed and efficiency, this tool really stands out when it comes to mass-testing. Always double check the results manually to rule out false positives.

Subjack will also check for subdomains attached to domains that don't exist (NXDOMAIN) and are available to be registered. No need for dig ever again! This is still cross-compatible too.

What's New? (Last Updated 09/17/18)

- Custom fingerprint support
- New Services (Re-added Zendesk && Added Readme, Bitly, and more)
- Slight performance enhancements

https://github.com/haccer/subjack
Subdomain takeover vulnerabilities

• We scanned around 3.5 million subdomains
• Around 0.5 % were potentially vulnerable
• Takeover through “AZURE Traffic Manager” was very successful
Subdomain Takeover by it.sec GmbH & Co. KG

it.sec

security for your information
Subdomain Takeover by it.sec GmbH & Co. KG

ice-rules-us.ccg.lenovo.com
Subdomain Takeover by it.sec GmbH & Co. KG

This page is secure (valid HTTPS).

- Certificate - valid and trusted
  The connection to this site is using a valid, trusted server certificate issued by COMODO RSA Domain Validation Secure Server CA.
  
- Connection - secure (strong TLS 1.2)
  The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_256_GCM (a strong cipher).

- Resources - all served securely
  All resources on this page are served securely.
**call.skype.com SSL certificate**

<table>
<thead>
<tr>
<th>SSL Product Type FQDN</th>
<th>Valid From</th>
<th>Valid To</th>
<th>Serial Number Status (Date)</th>
<th>Order # (Date)</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free SSL Certificate for call.skype.com</td>
<td>08-OCT-18</td>
<td>06-JAN-19</td>
<td>42D116BDB41C88EC9FA77925D555C71A Issued (08-OCT-18)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>177224777</strong> (08-OCT-18)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶ Download as .zip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>▶ Resend Invoice/Confirmation Email</td>
</tr>
</tbody>
</table>

16.11.2018  
it.sec GmbH & Co. KG  
19
Overview

• Subdomain takeover
• Exposed credentials
• Exposed source code
• Other interesting things
Don't put your `.env` files in the web-server directory:

```
db_password=

www.oneluxstudio.com/env

www.safeairtravels.com/env

www.oaksnorthaddison.com/env

https://github.com/codcasts/laravel/blob/master/.env

https://twitter.com/svblxyz/status/1045013939904532482
```

---

https://twitter.com/svblxyz/status/1045013939904532482
Exposed credentials

meg

meg is a tool for fetching lots of URLs but still being 'nice' to servers.

It can be used to fetch many paths for many hosts; fetching one path for all hosts before moving on to the next path and repeating.

You get lots of results quickly, but none of the individual hosts get flooded with traffic.

https://github.com/tomnomnom/meg
Exposed credentials

• We looked for .env files in the webroot
• We scanned only the Alexa Top 1 million without subdomains
• We identified
  • Hundreds of database passwords
  • PayPal API keys
  • Mail server credentials
  • ... and much more
Overview

• Subdomain takeover
• Exposed credentials
• Exposed source code
• Other interesting things
Don't publicly expose .git or how we downloaded your website's sourcecode - An analysis of Alexa's 1M

Sebastian participated in a CTF (capture the flag) a couple of months ago. One challenge he faced was the task of restoring a git repository from a directory listing enabled webserver. With directory listing, it was pretty easy, but Sebastian was curious if it’s possible to restore git repositories without directory listing and how common this misconfiguration flaw is.

With that idea in mind, we began to develop some tiny tools and started to do some research. The results were not as bad as anticipated, but nevertheless surprising.

TL; DR

Some websites host their version control repository (e.g. .git/) in production. Bad people can use tools to download/restore the repository to gain access to your website’s sourcecode. Check your webserver’s configuration now and make sure that it blocks access to these folders.

Exposed source code

• We checked all Alexa Top 1 million + subdomains (19 million ULRs) for exposed git repos (.git/ folders in the webroot)

• We found around 3900 sites to be vulnerable to this attack
  • Government sites
  • Big Austrian newspaper
  • Universities
  • and ....
Japan's cybersecurity minister admits he's never used a computer

"I give instructions to my aide."

BY SEAN KEANE | NOVEMBER 15, 2018 7:16 AM PST

Exposed source code

• [https://www.ebay.co.jp](https://www.ebay.co.jp) was vulnerable
  • Runs WordPress ?!
  • They leaked the complete WordPress source and more to unauthorized users
    • >1GB data
    • Database passwords
    • WordPress passwords
    • User uploads
    • and much more …
  • They fixed the issue within 10 hours!
Overview

• Subdomain takeover
• Exposed credentials
• Exposed source code
• Other interesting things
Other things we identified

- CORS misconfiguration
  - Microsoft (again ..)
  - Big Austrian telecommunication provider

- Open AWS S3 buckets
  - Terabytes of data – still investigating
  - We used „bucket-stream“ which scans transparency logs in real time
    - https://github.com/eth0izzle/bucket-stream
Lessons learned

• There are still tons of “low-hanging fruits“ out there
• You don’t need expensive super intelligent intrusion preventions systems if you don’t get the basics right
Future work

• Automate scans
• Use data of scans.io or Rapid7 project Sonar
• Eliminate false positives more efficiently
• Think about reporting issues more efficiently

https://scans.io
https://opendata.rapid7.com
Q&A
slashcrypto.org for the slides